Cliquez pour ajouter du texte

Cliquez pour ajouter du texte

THE NEOSHIELDS

DATA RISK MANAGEMENT & COMPLIANCE

PRÉSENTATION DU GROUPE THE NEOSHIELDS

Notre métier

THE NEOSHIELDS est aujourd'hui le seul acteur à exercer tous les aspects du métier autour du RGPD.

Un service 360 ° parce que pour nous, être au plus près des préoccupations de nos clients, c'est être en capacité de leur apporter une vue d'ensemble, des offres pertinentes, des outils agiles et innovants.

AUDITER :
accompagner votre entreprise pour inventorier vos activités de traitement, auditer votre conformité.

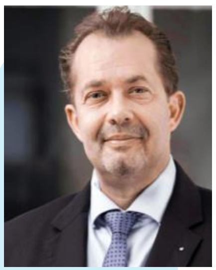
CONSEILLER :
guider la mise en place de votre organisation Informatique et Libertés et de vos procédures de conformité RGPD.

FORMER :
sensibiliser, former les collaborateurs, les dirigeants, les chefs de projet par le digital – en formation inter ou intra – pour DPO et Référent RGPD.

ACCOMPAGNER :
épauler le DPO interne d'une entité ou bien être le DPO Externe.
Dans les 2 cas nous outillons le DPO avec la solution de gouvernance PRIVACIL.

THE NEOSHIELDS, pionnier de la protection des données personnelles.

THE NEOSHIELDS, pionnier de la protection des données, est un acteur majeur du RGPD et de la Loi I&L depuis plus de 20 ans, Leader et innovant dans tous les domaines inhérents à la Protection des Données Personnelles.



2001 :
- Xavier Leclerc Président
1er DPO en France

2004 :
- 1ère société de Conseil et Audit en I&L
- Membre fondateur & Administrateur de l'AFCDP

2008 :
- 1ère société de logiciel SaaS de gestion de la Conformité I&L

2009 :
- Membre de l'European Advisory Board de l'IAPP (International Association of Privacy Professional)

2012 :
- 1er Label CNIL pour sa formation CIL
- 1ère homologation CNIL des procédures CIL mutualisées

2016 :
- 1er groupe français délivrant une offre complète de services RGPD

2017 :
- 1ère qualification Bureau Veritas pour sa certification DPO
- Fondation de l'UDPO (Union des DPO)

2018 :
- Renouvellement de l'ensemble des Labels CNIL pour ses formations pour 3 ans
- Lancement de l'offre Serious Game RGPD[4] en partenariat avec DAESIGN Interactive

2019 :
- Intégration des nouveaux référentiels CNIL au sein de la Plateforme Saas PRIVACIL
- Mise en place des nouvelles formations RGPD suivant les nouvelles préconisations CNIL de Mars 2019
- Co-fondation de l'EFDPO (Fédération Européenne des DPO)

2020 :
- Obtention du label indépendant PRIVACYTECH pour la conformité RGPD de la Plateforme de Gouvernance PRIVACIL

2021 :
- Obtention du label Intelligence Economique de la Région PACA

THE NEOSHIELDS, des références dans tous les secteurs et de toutes tailles

MÉTHODOLOGIE, MISSION OU COACHING DPO

Quatre étapes primordiales pour réussir sa conformité RGPD

1

Etat des lieux

2

Etablissement du Registre des Activités de Traitement, du Plan d'Action et des Études d'Impact sur la Vie Privée (EIVP / PIA)

3

Etablissement de la Gouvernance RGPD en interne / Formation des référents métiers

4

Internalisation ou externalisation du DPO

1

L'intérêt de l'état des lieux RGPD est de **concevoir des solutions** répondant aux exigences des règlementations en vigueur en matière de protection des données personnelles qui soient **cohérentes et personnalisées à l'ensemble des difficultés identifiées dans chaque service de votre structure**.

Ces solutions se veulent **pratiques** et ont pour objectif de ne pas entraver les collaborateurs dans l'exercice de leurs fonctions.

Un **état des lieux RGPD** tel que nous le proposons permet :

- **De faire une photo de départ ou état des lieux de la conformité de l'organisme au regard de la Loi « Informatique et Libertés » et du Règlement :**
- Pour chaque traitement
- De manière transverse (sécurité informatique, gestion du droit d'accès, …)
- **D'établir des livrables contenant :**
- Les non-conformités principales
- Des préconisations pour la mise en conformité
- Les règles à respecter (durées de conservation ou information des personnes par exemple)

Contrairement à un audit, nos revues de conformité se déroulent sur un mode déclaratif, et l'expérience montre que le processus est bien plus efficace (moins coûteux) et mieux ressenti en interne.

2

Pour donner suite à l'état des lieux RGPD, **THE NEOSHIELDS** rédigera les documents suivants :

Le registre des activités de traitements

Le **plan d'actions** (traitement, constat, action, priorité, recommandation personnalisée, service concerné, commentaires, …), véritable « feuille de route » de mise en conformité ainsi qu'une analyse des documents

Le **rapport de préconisations générales**

Les **fiches pratiques**

3

La Solution **PrivaCIL** est une Solution de Gouvernance RGPD, développée par nos experts métier en collaboration avec nos équipes de développement, dédiée pour les DPO et référents RGPD afin de gérer la conformité de leurs organismes au regard des lois relatives au traitement des données à caractère personnel.

PrivaCIL est une véritable Plateforme Saas de Gouvernance RGPD conforme aux exigences de la CNIL.

Public concerné :

La Solution **PrivaCIL** s’adresse à tous les organismes et toutes les personnes en charge de la gestion des données à caractère personnel :

- Responsable des Traitements (RT)
- DPO et réseau (référents RGPD)
- Responsable de la Sécurité des Systèmes d’Information (RSSI)
- Juriste / Avocat
- Profession Libérale
- Toute personne autorisée par l’un des précédents

10

4

Une fois l'état(s) des lieux RGPD réalisé(s), nous vous proposons de désigner **THE NEOSHIELDS** comme DPO externe ou de coacher le DPO Interne.

Le DPO Externe ou Interne a une fonction située au cœur de la conformité au règlement européen sur la protection des données (RGPD).

5 forfaits de 2 à 48 jours d'accompagnement ou de coaching par an avec la Plateforme de Gouvernance RGPD PRIVACIL incluse.

Le DPO est un chef d'orchestre chargé de conseiller et accompagner les organismes qui le désignent dans leur conformité.

FORMATIONS ET SENSIBILISATIONS RGPD

Si nous investissons autant de temps et d'expertise dans la conception de nos formations, c'est parce que la formation dans le domaine du RGPD est cruciale.

- D'abord, parce qu'elle permet d'imprégner les entreprises d'une culture RGPD vitale, donc de devenir responsable face à la réalité et aux enjeux de nos sociétés en matière de protection des données à caractère personnel.
- Mais plus encore, elle permet de rendre plus fort l'humain qui est souvent considéré dans le domaine du RGPD comme le maillon faible. Soit en formant des référents, des managers, des collaborateurs soit en permettant à chaque collaborateur d'une entreprise, d'une institution, d'une fédération etc. d'être sensibilisé, informé et formé à tous les enjeux liés au RGPD.
- Nous avons créé l'ensemble de nos formations en tirant la quintessence de nos 20 ans d'expérience. Mais aussi, en tenant compte de la réalité des différents publics concernés par ces questions. En pensant à toutes les situations que vous pouvez vivre dans votre vie professionnelle. Elles se veulent ainsi pragmatiques, didactiques, ludiques, opérationnelles, en un mot essentiel.

Certification de personnes
BUREAU VERITAS Certification
Délégué à la Protection des données

Qualiopi
processus certifié
RÉPUBLIQUE FRANÇAISE

La certification qualité a été délivrée au titre des catégories d'action suivante :
Actions de formation

apave
Certification

Formation du DPO

Objectifs de la formation :

- Connaître le cadre légal applicable en matière de traitement des données à caractère personnel
- Maitriser les principes et les obligations issues du Règlement Général sur la Protection des Données (RGPD) et de la Loi Informatique et Libertés
- Identifier les outils permettant de piloter une mise en conformité
- Développer une vision pragmatique et opérationnelle des impacts du RGPD
- Connaître les risques liés à la non-conformité

Formation des Référents > Les collaborateurs de l'entreprise en lien avec le DPO

Objectifs de la formation :

- Acquérir les connaissances et les compétences nécessaires à la fonction de référent RGPD
- Maîtriser les obligations du RGPD
- Être un interlocuteur performant dans la démarche de conformité de l'entreprise et au sein du réseau Informatique et Libertés

L'offre de formations RGPD THE NEOSHIELDS multimodales en digital vous aide à déployer les compétences utiles et à synchroniser vos équipes en vue de mettre en conformité les fonctions de votre entreprise avec le RGPD, mais aussi d'en faire un atout économique, commercial et d'organisation.

Ces outils e-learning et Serious Game ont été développé en collaboration avec un acteur majeur du marché spécialiste, filiale du Groupe NATHAN, la société DAESIGN.

Notre offre à été soutenue et labellisée par nos OPCA (OPCO) partenaires

Contactez votre conseiller habituel OPCO pour échanger sur le format de formation adéquat et les financements adaptés à mettre en place

OPÉRATEUR DE VOS COMPÉTENCES

L'humain au cœur des services

PARTENAIRE DE VOS COMPÉTENCES

- **Tarif soumis à devis suivant le nombre de licence digital souscris (nombre de collaborateurs à former).**
- **Des prix dégressifs**

- Contenus complets et 100% conformes au RGPD
- Offre adaptée à tous les profils de l'entreprise
- Attestation de formation en fin de parcours
- Accessible via notre ou votre plateforme LMS
- Application mobile pour réactiver ses connaissances

Différents parcours disponibles :

RGPD 20 MINUTES

RGPD L'AFFAIRE DE TOUS (1H30)

TOP MANAGEMENT (2H)

RGPD DE A À Z (4H)

PLATEFORME DE GOUVERNANCE RGPD – SOLUTION SAAS PRIVACIL

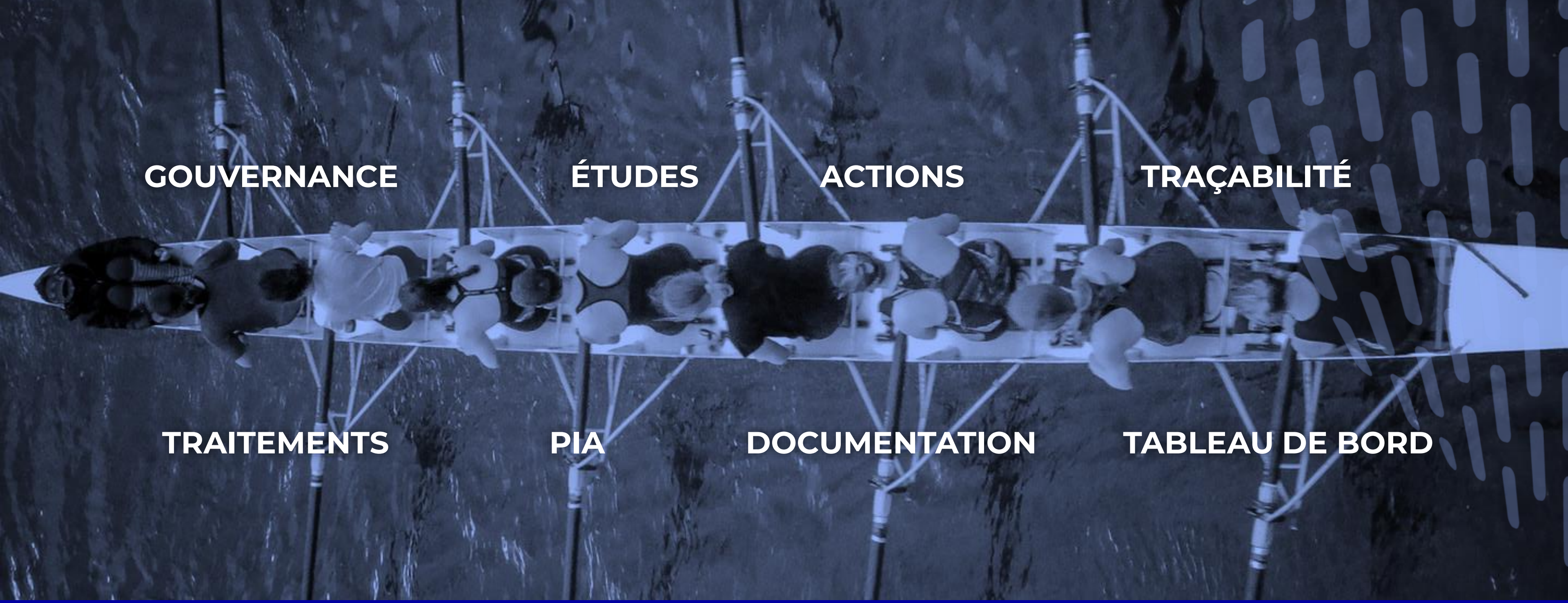
PrivaCIL apporte, en plus des éléments de base que sont la tenue du registre, la gestion des actions de suivi, la gestion des demandes et des droits (accès, rectification, opposition, consentement, portabilité, oubli (internet), la mise en place d'audit de conformité, et tout un ensemble de fonctionnalités dans un contexte de workflow quelle que soit la taille de l'organisme ou son secteur d'activité :

- Gestion du Registre des Traitements
- Gestion du Registre des Sous-Traitants
- Gestion des études d'impact sur la vie privée (EIVP / DPIA)
- Audit/évaluation de conformité des traitements
- Bilan annuel du DPO
- Gestion des demandes de droits
- Gestion des notifications de failles de sécurité
- Gestion de l'accountability
- Gestion des analyses de risques au niveau Entreprise
- Suivi des actions correctives avec plan d'actions DPO

PRIVACIL A OBTENU LE LABEL **PRIVACY TECH** POUR L'EXCELLENCE DE SA PLATEFORME DE GOUVERNANCE RGPD EN MATIÈRE DE PRIVACY RGPD.

Public concerné

8 outils au service des acteurs de la conformité



General Data
Protection Regulation

PrivaCIL s’inscrit dans le cadre du règlement européen (RGPD/GDPR) afin d’offrir aux organismes la possibilité de répondre aux exigences depuis le 25 mai 2018.

Une solution orientée métier :

- Workflow intégré (DPO, Référent RGPD, RSSI, RT, Chefs de projet)
- Reporting complet
- Accountability
- Label Gouvernance

Une architecture extensible :

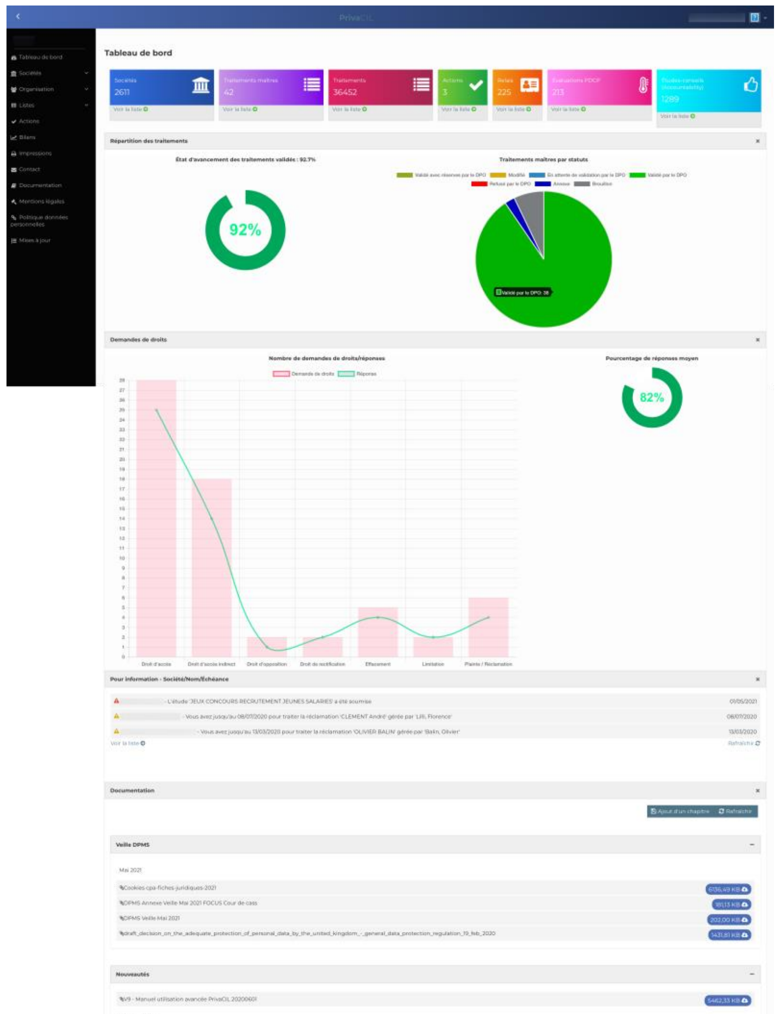
- Mode SaaS
- Infrastructure évolutive
- Multi langues
- Données sécurisées
- Coûts maîtrisés

Des fonctionnalités techniques :

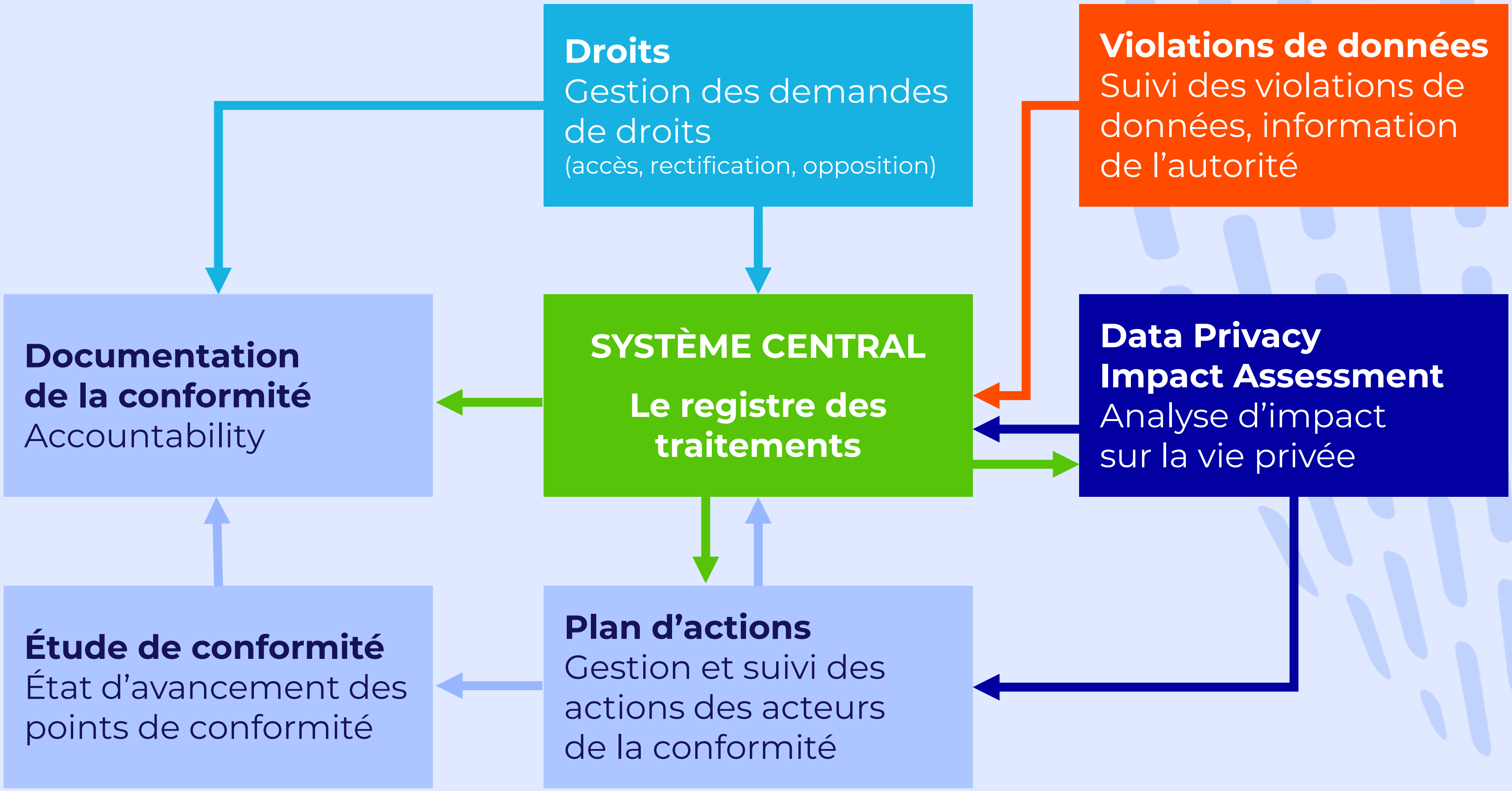
- Gestion des Utilisateurs
- Gestion des délégations
- Traçabilité globale
- Gestion des sauvegardes
- Portabilité entrante et sortante

Le tableau de bord (Dashboard)

- Le tableau de bord est le point central de la Solution, il fournit à l’utilisateur une synthèse de la situation de l’organisme au regard de ses tâches de conformité et permet d’accéder directement aux actions à mener en priorité.



Couverture fonctionnelle



MONITORING COOKIES & TRACEURS

Une augmentation significative des notifications d'infraction

Plus de trois ans se sont écoulés depuis la première application du RGPD (mai 2018).
La tendance actuelle des notifications d'infraction continue de connaitre une croissance à deux chiffres et risque de continuer à augmenter au fil des années.

> PLUS DE 281 000 NOTIFICATIONS D'INFRACTION DEPUIS MAI 2018

331 NOTIFICATIONS/JOUR EN MOYENNE EN 2020
HAUSSE DE 19% PAR RAPPORT À 2019

En France, une évolution stable du nombre de notifications de violations de données avec toujours des manquements pour avertir les personnes

4 737 notifications reçues par la CNIL entre l'entrée en application du RGPD et juillet 2020.

61% des notifications impactent moins de 300 personnes et seulement 13% impactent plus de 5000 personnes.

Les secteurs les plus touchés sont le secteur **scientifique**, la **finance** et l'**administration publique.**

77% des personnes impactées par les fuites n'ont pas été averties.

55% des pertes ont pour origine des actes malveillants

90% des pertes impliquent des pertes de confidentialité

Les pertes de données sont en majorité d'origine malveillante (piratage, phishing), en nette augmentation par rapport au bilan 2019 où les pertes étaient d'origine accidentelles. La perte de confidentialité (accès aux données par des personnes non autorisées) est toujours majoritaire, en plus de la perte de l'intégrité (modification non autorisée des données), la perte de disponibilité (perte d'accès ou destruction accidentelle des données) apparaît désormais.

Source: CNIL.

Une augmentation significative des notifications d'infraction (2)

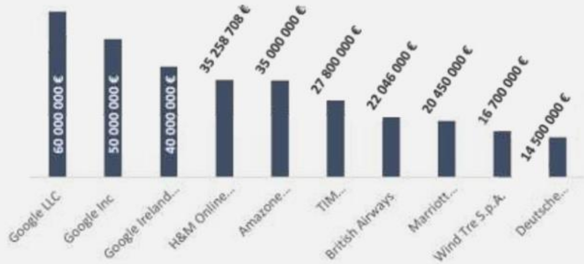
Des sanctions en nette augmentation, avec de grandes disparités entre les pays

494 sanctions pécuniaires RGPD (près de **409,5 M€**) prononcées par les autorités locales en EU, à l'encontre d'entreprises à travers le monde (dont aux USA) après 2 ans ½

Depuis janv.2020: 339 sanctions, soit 187,2M€

14 sanctions pécuniaires, soit près de **189,4 M€** d'amendes publiques appliquées par la CNIL dans le cadre du RGPD en France

Principales sanctions pécuniaires dans le cadre du RGPD



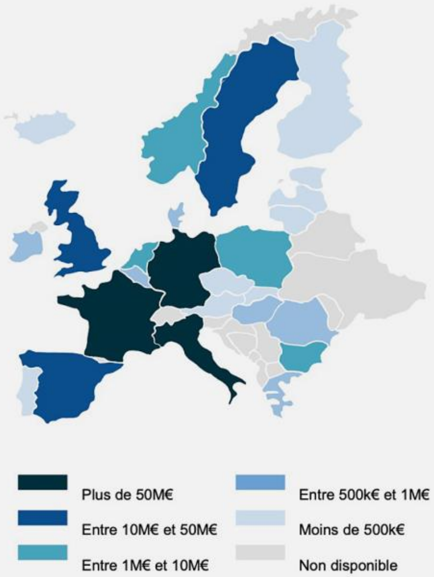
41%

des sanctions sont dues à une base légale du traitement des données insuffisante

22%

des sanctions sont dues à une insuffisance des mesures techniques et organisationnelles pour garantir un niveau de sécurité adapté au risque

Amendes cumulées par pays en Europe

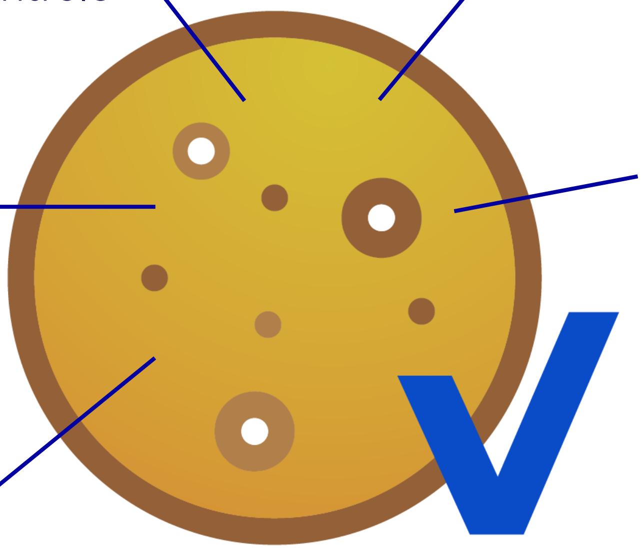


Sources: GDPR CNIL.

Les avantages de la mise en conformité des cookies

Réduire au minimum la sanction possible de l'autorité de contrôle

La donnée est donc plus rare et a une valeur plus importante sur le marché



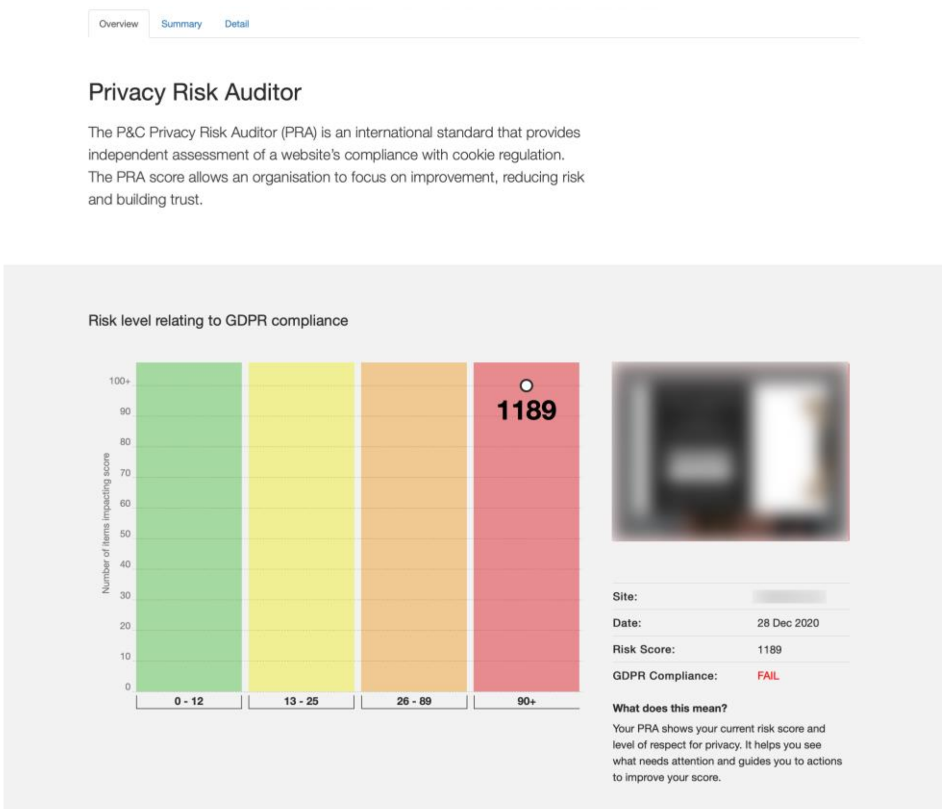
Augmentation de la qualité des données collectées avec consentement

Une base de données plus qualitatives augmente le coût par mille (CPM)

La qualité de la donnée ciblée augmentée

Monitoring Score Privacy-Annuel

- Calcul du Score Privacy et détail des cookies devant être analysés.
- Le Score Risque RGPD Cookie est la norme internationale pour signaler l'impact de l'utilisation de cookies non consensuels et des technologies de suivi associées.
- Le score fournit aux DPO une compréhension instantanée et indépendante de leur position de risque et une base de référence à partir de laquelle l'amélioration peut être suivie.
- Le Score Risque RGPD Cookie est un calcul mathématique qui prend en compte le nombre, la catégorisation et l'impact sur la confidentialité des cookies et des objets de stockage Web définis sur un site Web donné. Il n'y a pas de subjectivité dans le calcul, l'intelligence automatisée est utilisée pour identifier les cookies qui sont définis avant que le consentement ne soit donné librement.



Prix dégressif suivant le nombre de sites, nous contacter

AUDIT Cookies I RGPD-4 SEMAINES

Semaine 1

Pré audit
avec calcul du score Privacy Cookies et détail des cookies détectés

Semaine 2

Workshop 1
Cookies et RGPD

Semaine 3

Workshop 2
Analyse des cookies - Priorisation

Semaine 4

Workshop 3
Actions et solutions de remédiation

Audit final
avec calcul du score Privacy Cookies et détail des cookies restants

1 an

Monitoring
sur 12 mois inclus

OFFRES CYBERSÉCURITÉ

La Cybersécurité en quelques chiffres

92%

Des entreprises européennes (ETI et grands groupes) ont déjà subi des incidents de cyber-sécurité au cours des 5 dernières années

84%

(51 % de PME) des entreprises françaises ont déjà été victimes de vols d'informations.
Le montant des pertes enregistrées (arrêt d'exploitation, cout de remédiation, etc.) varie entre 750 000 € et 1,1 M€.

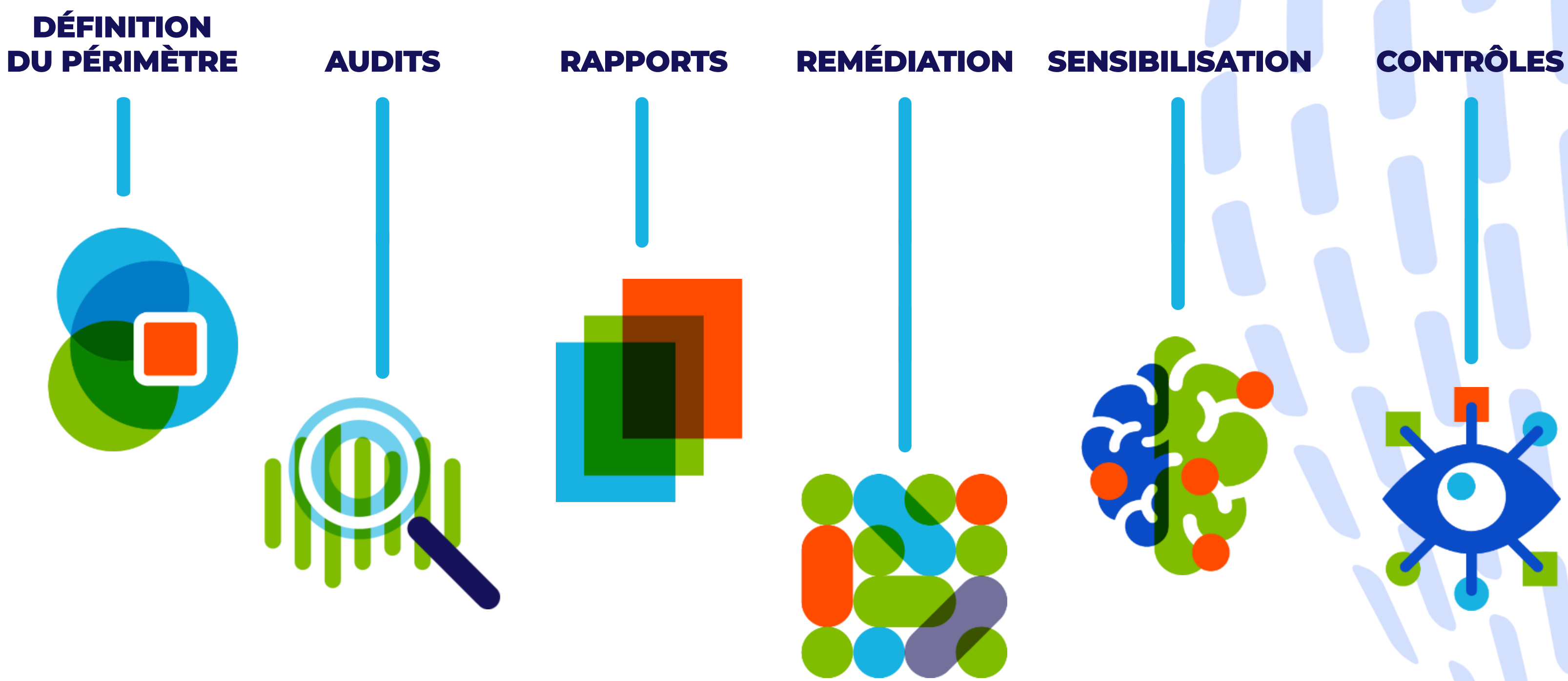
35%

Des incidents sont générés, malgré eux, par des collaborateurs

Réparations des dégâts d'une cyberattaque

9 : semaines nécessaires (en moyenne)
800 000 € : budget estimé (en moyenne)

Notre méthodologie



CATALOGUE OFFRES CYBERSÉCURITÉ

Cartographie des Systèmes d'information

• Du fait des interconnexions, de la complexification et de l'externalisation des systèmes d'informations, les réseaux deviennent difficiles à appréhender.

• Pour couvrir toute l'architecture technique, **THE NEOSHIELDS** propose deux types de cartographie :

• Une cartographie « offensive » des ressources réseau ouvertes à l'extérieur sans connaissance préalable du système d'information. Dans cette démarche, une simulation de prise d'empreinte réalisée par les pirates en amont de leurs offensives technique est réalisée.

• Une cartographie complète du réseau (lan, wan, accès internet, redondance, flux, ...). si l'expertise et la réalisation du réseau sont en partie ou entièrement externalisées, **THE NEOSHIELDS** peut intervenir pour réinternaliser la connaissance et la maîtrise du réseau.

Audit interne

• L'audit interne permet de simuler les agissements d'une personne malintentionnée qui a obtenu un accès au réseau interne de la cible.

• Cet audit évalue la sécurité d'un système d'informations (si) dans plusieurs situations réelles :
- Stagiaire ou employé malintentionné ou négligent
- Mauvaise configuration du périmètre
- Attaquant ayant réussi à pivoter dans le réseau interne depuis l'extèrieur

• Le périmètre d'intervention est défini avec le client avant toute mission d'audit. Ensuite, il s'agit d'identifier les problèmes liés à l'infrastructure informatique, à la sécurité des postes de travail, aux services jugés annexes peu ou mal sécurisés, aux défauts de cloisonnements des environnements, aux mauvaises configurations, etc ...

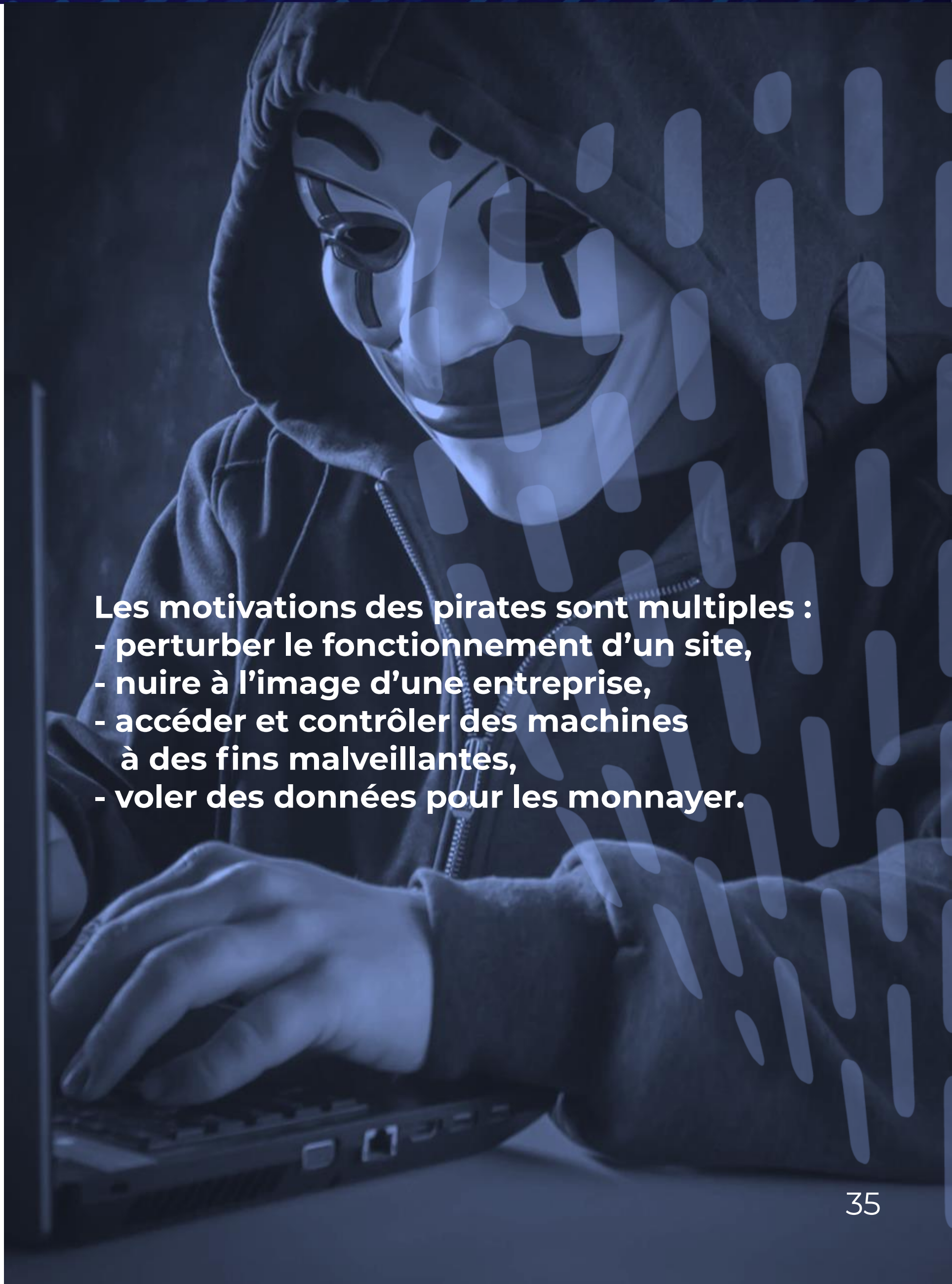
Audit externe

• Cet audit permet d'évaluer la vulnérabilité d'un SI face à un attaquant externe qui n'a pas de « connaissance à priori » de la cible. Cet audit est réalisé séparément de l'audit interne dont il complète les résultats.

• L'objectif est alors de simuler les agissements d'un pirate qui va dans un premier temps chercher à approfondir sa connaissance si pour ensuite exploiter des vulnérabilités techniques et au final :

- Accéder à des informations sensibles confidentielles (métier, mails, ...)
- Prendre le contrôle d'une ressource
- Accéder au réseau interne

• Lors de ces tests, plusieurs éléments sont évalués comme la robustesse des machines, des softwares, la sécurité des services et applications, les éléments de sécurité périmétriques, la sécurité des systèmes d'authentifications, ...



Audit intrusion – Red Team

• Le test d'intrusion en mode « red team » se veut une mise en situation la plus proche possible de la réalité.

• Plus long et d'un périmètre plus large que les tests classiques d'intrusion, son objectif est de simuler une attaque ciblée réaliste en intégrant aux attaques techniques les scénarios d'intrusion physique d'une part et de l'ordre de l'ingénierie sociale d'autre part.

• Plusieurs vecteurs d'attaques physiques ou utilisant des « failles humaines » peuvent être envisagés :

- Envoi d'email malveillants (phishing, pièce jointe contenant un malware, …)
- Ingénierie sociale sur les équipes et le personnel
- Intrusion physique afin de connecter un implant sur le réseau ou créer un faux point d'accès internet.

• Ce type d'audit permet d'évaluer, en plus de l'architecture informatique, la sensibilisation et la réactivité des équipes face aux attaques ainsi que la remontée d'alertes en interne.

Conseil et Formation

- **THE NEOSHIELDS** accompagne ses clients durant toutes les phases de mise en place ou d'amélioration de la sécurisation de leur système d'informations.

- Il peut être proposer les thèmes suivants :

▪ Une analyse des besoins de sécurité
▪ Une aide dans le choix des produits de sécurité
▪ Une analyse de risques, la mise au point de politiques de sécurité et la mise en place de votre plan de continuité d'activité
▪ Des formations afin d'aider le personnel et ou la direction générale à anticiper, à identifier et à réagir de façon adaptée aux menaces, incidents ou alertes de sécurité et appliquer les bonnes pratiques.

- Pour atteindre leurs objectifs, une majorité des attaques exploitent le facteur humain. C'est pour cette raison que les conseils et la formation sont essentiels pour une prévention et une protection efficaces.

Gestion de crise

• THE NEOSHIELDS propose un accompagnement au plus près lors d’une urgence suite à un incident de sécurité.

• Selon la nature de ce dernier, nos consultants pourront être amenés à :

- Identifier la source de l’intrusion / forensic
- Effectuer un état des lieux et des systèmes
- Mesurer l’étendue de l’attaque et la stopper
- Récupérer les données et s’assurer de l’intégrité du SI afin d’en assurer le redémarrage rapide
- Formuler des recommandations préventives et correctives

• Pour atteindre leurs objectifs, une majorité des attaques exploitent le facteur humain. C’est pour cette raison que les conseils et la formations sont essentiels pour une prévention et une protection efficace.

Investigation Web

- Identifier, cartographier des sites, blogs, forums, ... sur le web présentant un intérêt ou une menace particulière.

- Récolter dans la mesure du possible le maximum d'information sur l'écosystème technique, organisationnel, juridique, financier et définir des indicateurs ou outils de mesure de l'activité de ces derniers.

- Surveiller ces lieux d'échanges marchand ou non pour détecter toutes évolutions, modifications de leur organisation ou proposition.

- Proposer sur les bases des informations récoltées et des constats effectués des recommandations d'actions.

Usurpation d’email

- Les experts THE NEOSHIELDS utilisent leurs outils uniques de diagnostic pour corriger les failles de sécurité de l’usage des emails par des tiers.

Cette prestation inclut :

- Suivi personnalisé des échanges avec les différents interlocuteurs techniques
- Communication de documents techniques référents et standardisation des échanges
- Envoi régulier par mail de rapport statistique DMARC avec les IP impliquées dans les envois : inclus dans la gestion d’un nom de domaine défensif
- Surveillance quotidienne de la configuration email adaptée (securl)
- Analyse humaine des rapports DMARC

PLATEFORME DE GESTION DES ALERTES PROFESSIONNELLES

Un partenariat avec l'acteur N°1 en Europe

THE NEOSHIELDS est partenaire avec **EQS Group**, acteur majeur de la compliance en Europe, pour manager le traitement des Alertes Professionnelles, activité de traitement devant être inscrites au Registre des activités de traitement **pour les sociétés de plus de 50 salariés**, comme l'impose la Directive Européenne sur la protection des lanceurs d'Alerte.

Quelles sont les exigences de la **Directive Européenne sur la protection des lanceurs d'alerte** ?

Mettre en place un canal de signalement.

Devoir de confidentialité des lanceurs d'alerte

Il est essentiel de veiller à ce que l'identité des lanceurs d'alerte reste confidentielle afin d'éviter d'éventuelles représailles.

Hébérgement sécurisé des données

La plateforme de signalement doit être protégée et sécurisée.

Conforme au RGPD

Toutes les données personnelles doivent être utilisées et traitées conformément au RGPD.

Délais de réponse au lanceur d'alerte

Le lanceur d'alerte doit obtenir une réponse dans un délai maximum de 7 jours. Le lanceur d'alerte doit être informé des mesures prises, de l'état d'avancement de l'enquête interne et du résultat dans un délai de 3 mois.

Obligation d'informer les employés sur les options possibles pour signaler un comportement non éthique

Ces informations doivent être facilement accessibles et compréhensibles. Cela s'applique également aux parties prenantes, aux fournisseurs, aux partenaires commerciaux et aux prestataires de services.

Communication sur le canal de signalement externe (autorités compétentes)

Les entreprises doivent communiquer sur l'ensemble des canaux de signalement proposés aux employés qu'ils soient internes ou externes.

Votre dispositif d'alerte interne ne sera performant **que s'il protège efficacement vos employés**

PROTÈGE LES EMPLOYÉS

- La volonté de fournir des informations sensibles augmente
- La peur des représailles diminue

RÉDUIT LES COÛTS

- En prenant des mesures préventives
- Permet une détection à un stade précoce des comportements non éthiques

MINIMISE LES RISQUES

La détection à un stade précoce de ces comportements non éthiques permet de réduire :

- Les risques financiers
- Les risques de responsabilité
- Les risques réputationnels

3 principaux challenges concernant les signalements

MANQUE D'INFORMATION

Les employés ne savent pas auprès de qui et comment signaler un comportement non éthique de manière sécurisée.

SURCHARGE DE TRAVAIL

Les entreprises manquent de temps pour la mise en place d'un canal de signalement fiable, efficace et conforme aux lois en vigueur.

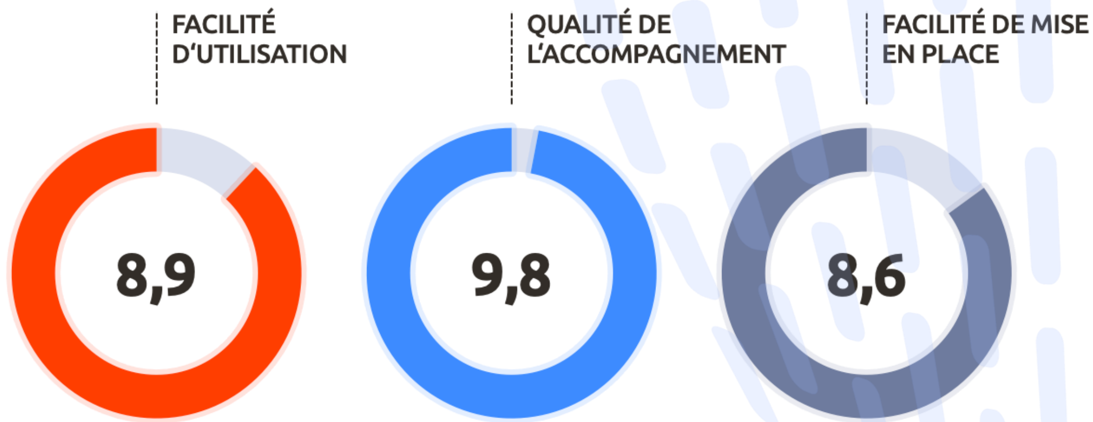
DÉCENTRALISATION

Pas de vue d'ensemble et centralisée des signalements et documentation insuffisante.

EQS Integrity Line – **Le dispositif d'alerte interne de référence dans l'Union Europeénne**

Avec près de **1000 clients**, EQS Integrity Line est la plateforme de lancement d'alerte la plus utilisée dans l'UE.

- Expert en plateforme de recueil et de traitement des alertes depuis 2009
- Des solutions adaptées à la taille et aux besoins de l'entreprise
- Disponible en plus de 70 langues
- Hébergée en Allemagne
- Haute sécurité et tests d'intrusion réguliers (ISO 27001)
- Conforme au RGPD



La plateforme EQS Integrity Line : **sécurisée et certifiée**

24/7

Le lanceur d'alerte peut signaler un comportement non éthique de manière sécurisée et anonyme 24h24 et 7j/7 et dans la langue de son choix.

Les gestionnaires de cas traitent les alertes de manière centralisée et communiquent en toute confidentialité avec le lanceur d'alerte.

Toutes les alertes sont cryptées et hébergées sur des serveurs
hautement sécurisés et certifiés ISO 27001.

Protection des données et sécurité des informations

DES TECHNOLOGIES DE CRYPTAGE MODERNES

Notre cryptage avancé garantit qu'aucun tiers - y compris EQS Group - n'a accès à vos données.

TEST SUR NOTRE SOLUTION CONTRE LES ATTAQUES PAR FORCE BRUTE

Un audit externe de sécurité confirme le très haut niveau de sécurité de nos solutions.

CERTIFICATION DIGICERT SSL

HTBridge a attribué la note A+ à notre sécurité SSL.

PARE-FEU ET RESTRICTIONS IP

Nous utilisons les dernières technologies en matière de pare-feu et de restrictions IP pour protéger les systèmes contre les attaques.

PROTECTION DES FICHIERS AVEC FILE DETOX

Nous nettoyons toutes les pièces jointes avec File Detox, évitant ainsi que des virus, même de type "0-day", n'atteignent nos serveurs et vos données.

ANONYMAT

Pour garantir l'anonymat, nous veillons à ce qu'aucune adresse IP ou horodatage ne soient stockés dans le système.

PROTECTION DES ATTAQUES PAR FORCE BRUTE

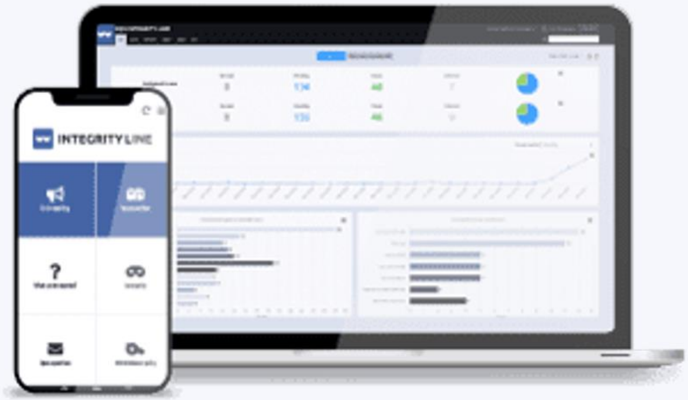
Les attaques cryptanalytiques sont fréquentes dans les attaques de systèmes. Nous utilisons la méthode de cadenassage pour prévenir les attaques par force brute.

AUTHENTIFICATION À 2 FACTEURS

La méthode d'authentification à 2 facteurs permet de prévenir les vols d'identité. Personne ne peut donc se connecter avec vos codes d'accès.

Les avantages d'EQS Integrity Line

- Hébergement sécurisé de vos données en Allemagne
- Certifiée ISO 27001 et conforme au RGPD
- Une plateforme simple et intuitive pour le lanceur d'alerte
- Personnalisation en fonction de vos besoins
- Anonymat garanti du lanceur d'alerte
- Disponible dans plus de 70 langues
- Statistiques et analyses de données détaillées
- Plateforme clé en main avec des fonctionnalités standards de haute qualité



Signalement simple, intuitif et sécurisé

- **Vos données sensibles parfaitement sécurisées** avec les techniques de cryptage et les certificats SSL
- Module de dialogue sécurisé et confidentiel avec **possibilité pour le lanceur d'alerte de rester anonyme**
- Signalement possible depuis n'importe quel appareil (smartphone, tablette ou PC)
- **Conforme aux directives d'accessibilité pour le Web**

Module intégré de gestion des cas: traitement des alertes, collaboration et communication avec vos équipes

- Une plateforme **multilingue** pour une utilisation dans le monde entier avec un **service de traduction automatique intégré**
- **Droits et autorisations individuels**
- **Statistiques et analyses de données détaillées** avec les fonctions de recherche et de filtre
- Possibilité **d'inclure des alertes provenant d'autres canaux de signalement** ex : E-mail, téléphone, courrier
- **Charte graphique personnalisée** ex : couleurs, logo

Interconnexion entre THE NEOSHIELDS et EQS Group

La plateforme de Gouvernance RGPD de **THE NEOSHIELDS** et la plateforme de Gestion des Alertes Professionnelles **d'EQS Group** dialoguerons intelligemment ensemble pour faire état au Responsable Conformité et Compliance d'un organisme des nouvelles alertes pouvant avoir une interaction avec le RGPD et la Gestion des Alertes Professionnelles.

OFFRE LOI SAPIN II - ANTICORRUPTION

Renforcement du dispositif de prévention et détection des risques d’atteinte à la probité

1 Mettre en place des sessions de formations / sensibilisations en lien avec le COMEX et à partir du risque sectoriel

Cette démarche s'articulera sur 3 types de formations (10 personnes par sessions) par rapport à l'exposition aux risques du personnel

> Préparation du Support COMEX
- Présentation en ligne et échanges avec le COMEX (1h30)

> Formation / Intervention en ligne pour le personnel à risque
- Par groupe de 10 personnes
- Session de 7h

> Formation / Intervention en ligne pour le personnel à risque
- Par groupe de 10 personnes
- Session de 3h

> Sensibilisation en ligne à la prévention de la corruption
- Par groupe de 20 personnes
- Session de 1h

Livrables
Support de formations > Tests et corrections > Bilan de fin de session

2 Élaboration d'une cartographie des risques d'atteinte à la probité

Permettra d'identifier l'univers de risques de la société, de les hiérarchiser selon des critères d'impact et de probabilité d'occurrence et de déterminer les mesures de prévention et détection à déployer prioritairement

La démarche de cartographie, construite sur la base des recommandations de l'Agence Française Anticorruption, s'organisera en 6 étapes :

1 > Élaboration de la méthode

- Définition et validation du périmètre d'application et des éventuelles exclusions
- Définition des rôles et responsabilités des parties prenantes à la cartographie (RACI)
- Définition des critères d'impact, d'occurrence, les facteurs aggravants, les outils

2 > Identification des processus exposés

- Sur la base des critères d'exposition aux risques : interactions avec les tiers et enjeux

3 > Animation des entretiens/groupes de travail sur les processus exposés pour identifier et coter les risques bruts

- Identification des scenarii de risques
- Cotation des risques bruts (impact x occurrence x facteur aggravant)

4 > Réévaluation des risques bruts en tenant compte des mesures de prévention existantes

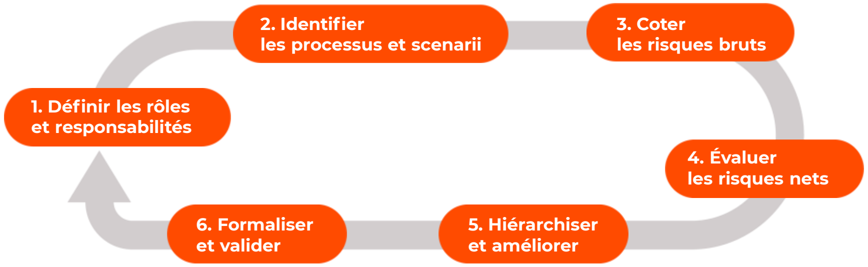
- Évaluation des mesures de maîtrise des risques
- Cotation des risques nets (réévaluation du risque brut après application des mesures de maîtrise)

5 > Stratégie de gestion des risques

- Revue des scenarii : hiérarchisation et harmonisation
- Détermination de la limite d'acceptabilité
- Élaboration des plans d'actions et modalités de suivi (acteurs, fréquence, indicateurs)

6 > Formalisation et diffusion

- Organisation par compétence, métier, processus
- Validation par l'instance dirigeante, présentation aux comités non exécutifs, communication interne



Livrables

Cartographie des risques d'atteintes à la probité ainsi que l'ensemble des supports de la démarche (guide méthodologique, comptes rendus d'entretien, grilles de cotation des risques, stratégie de gestion des risques, plans d'actions), participation aux groupes de travail

3 Accompagnement dans la construction du dispositif de maîtrise des risques selon les plans d'actions déterminés lors de la cartographie

Conformément aux recommandations de l'AFA, la construction du dispositif de maîtrise des risques d'atteinte à la probité s'articulera autour :

> **Du code de conduite :** accompagnement dans la conception et la rédaction du code de conduite et conception du plan de communication interne associé

> **Du dispositif d'évaluation des tiers :** co-construction du dispositif (sur une base 50/50) comprenant l'identification des tiers, leur exposition aux risques d'atteintes à la probité, la conception des outils d'évaluation selon les différents niveaux de contrôle possibles (du contrôle juridique et financier à la due diligence externe), la rédaction de la procédure associée

> **De l'alerte interne :** assistance à la rédaction du cahier des charges et à l'identification des prestataires externes, conception du plan de communication interne

> **Des dispositifs de contrôle interne :** accompagnement dans l'identification des contrôles existants et la rédaction d'un manuel de contrôle interne spécifique anticorruption, comprenant les contrôles comptables

> **Des mesures correctives :** construction des outils de pilotage du dispositif (indicateurs de pilotage et de suivi)

> **Régime disciplinaire :** revue du régime existant et propositions d'évolution au regard des recommandations de l'Agence Française Anticorruption

Livrables
Code de conduite, procédure d'évaluation des tiers, cahier des charges de l'alerte interne, manuel de contrôle interne spécifique anticorruption, outils de pilotage du dispositif, propositions d'évolution du régime disciplinaire

www.theneoshields.eu

THE NEOSHIELDS
1200, avenue du Dr Maurice Donat – Natura 3
06250 MOUGINS - FRANCE

Office : +33 (0)4 97 97 34 31
Contact : gestionclients@theneoshields.eu